MUNICIPALIDAD DE SAN JOAQUÌN
DIRECCIÓN JURÍDICA

DECRETO Nº 2701 /
Sección 1ª

SAN JOAQUÍN 29 DIC 2017

LA ALCALDÍA DE SAN JOAQUÌN, DECRETÓ HOY LO SIGUIENTE:

VISTOS: 1) Decreto Alcaldicio N° 2938 de fecha 30.12.2016 que aprueba el Programa de Mejoramiento de la Gestión municipal para el año 2017, correspondiente al PMG-2017 Unidad de Dirección de Gestión administrativa, en su Objetivo N°3 e indicador N°3, decretar manual Políticas de Seguridad y Respaldo de Información; 2) Memo N°8, metas colectivas con fecha 28 de Julio de 2017, Borrador Políticas de Seguridad y Respaldo de Información; 3) Providencia 492 de fecha 28 de diciembre de 2017 que instruye decretar Manual de Seguridad y Respaldo de Información; y

TENIENDO PRESENTE: Las facultades que me confiere la Ley 18.695 Orgánica Constitucional de Municipalidades, especialmente lo dispuesto en sus artículos. Nº 63 y 65, cuyo texto refundido fue fijado por el DFL -1 del, Ministerio del Interior, del 26 de julio de 2006.

DECRETO:

1.- APRUÉBASE el Manual de Políticas de Seguridad y Respaldo de Información.

2.- Déjese constancia que este Manual debe ser revisado y ajustado a lo menos cada 6 meses por el Departamento de Informatica.

ANÓTESE, COMUNÍQUESE, CÚMPLASE

Y ARCHÍVESE.

MUNICIPALIDAD DE SAN JOAQUIN
SECRETARIO MUNICIPAL
ERIC LEYTON RIVAS
SECRETARIO MUNICIPAL

MUNICIPALIDAD DE SAN JOAQUIN
ALCALDE
GERARDO SANCHEZ GALLARDO
ALCALDE (S)

Departamento de Informática
Municipalidad de San Joaquín

Políticas de Seguridad

y

Respaldo de Información

Santiago 27 de Diciembre de 2017

I. Justificación

Los activos de información y los equipos informáticos son recursos importantes y vitales para toda la Municipalidad. Sin ellos se quedarían rápidamente fuera de un servicio a la comunidad y por tal razón la Administración tiene el deber de preservarlos, utilizarlos y mejorarlos. Esto significa que se deben tomar las acciones apropiadas para asegurar que la información y los sistemas informáticos estén apropiadamente protegidos de muchas clases de amenazas y riesgos tales como fraude, sabotaje, espionaje, extorsión, violación de la privacidad, intrusos, hackers, interrupción de servicio, accidentes y desastres naturales.

La información perteneciente a la Municipalidad debe protegerse de acuerdo a su valor e importancia. Deben emplearse medidas de seguridad sin importar cómo la información se guarda (en papel o en forma electrónica), o como se procesa (PC`s, notebook's, servidores, etc.), o cómo se transmite (correo electrónico). Tal protección incluye restricciones de acceso a los usuarios de acuerdo a su cargo.

Cuando ocurra un incidente grave que refleje alguna debilidad en los sistemas informáticos, se deberán tomar las acciones correctivas rápidamente para así reducir los riesgos.

II. Generalidades

Está política debe ser comunicada a todos los funcionarios de la municipalidad, de una forma apropiada, accesible y entendible para el lector.

Objetivo

La Municipalidad debe tener vigente una política de seguridad informática que le permita establecer un marco para la implantación de seguridad y control extensivo a todas las áreas.

Alcance

Está política se aplica a toda la Municipalidad de San Joaquín, rige para todos los usuarios de sistemas y el personal externo.

Responsabilidades

Los siguientes entes son responsables, en distintos grados, de la seguridad en la municipalidad:

1. **Comité de Informática.-** Será conformado por la Directora de Gestión Administrativa o quien le subrogue, el Jefe de Seguridad o encargado del Departamento de Informática y el encargado de Servidores y redes. Este comité será responsable de implantar y velar por el cumplimento de las políticas, normas, pautas, y procedimientos de seguridad a lo largo de toda la organización, todo esto en coordinación con el Administrador Municipal. También es responsable de evaluar, adquirir e implantar productos de seguridad informática, y realizar las demás actividades necesarias para garantizar un ambiente informático seguro. Además debe ocuparse de proporcionar apoyo técnico y administrativo en todos los asuntos relacionados con la seguridad, y en particular en los casos de infección de virus, penetración de hackers, fraudes y otros percances.

2. **Jefe de Seguridad o encargado de Informática.-** Es responsable de dirigir las investigaciones sobre incidentes y problemas relacionados con la seguridad, así como recomendar las medidas pertinentes.

3. **Encargado de Servidores y Red.-** Es responsable de establecer los controles de acceso apropiados para cada usuario, la creación de nuevos usuarios, supervisar el uso de los recursos informáticos, administrar la red, revisar las bitácoras de acceso y de llevar a cabo las tareas de seguridad relativas a los sistemas que administra. El Encargado de Servidores y Red también es responsable de informar al Jefe de Seguridad o encargado de Informática sobre toda actividad sospechosa o evento insólito.

4. **Usuarios.-** Son responsables de cumplir con todas las políticas de la Municipalidad de San Joaquín relativas a la seguridad informática y en particular:
   - Conocer y aplicar las políticas y procedimientos apropiados en relación al manejo de la información y de los sistemas informáticos.
   - No divulgar información confidencial de la compañía a personas no autorizadas.

- No permitir y no facilitar el uso de los sistemas informáticos de la Municipalidad de San Joaquín a personas no autorizadas.
- No utilizar los recursos informáticos (hardware, software o datos) y de telecomunicaciones (teléfono, celulares) para otras actividades que no estén directamente relacionadas con el trabajo en la Municipalidad de San Joaquín.
- Proteger meticulosamente su contraseña y evitar que sea vista por otros en forma inadvertida.
- Seleccionar una contraseña fuerte que no tenga relación obvia con el usuario, sus familiares, el grupo de trabajo, y otras asociaciones parecidas.
- Reportar inmediatamente a su jefe directo o a un funcionario del Departamento de Informática cualquier evento que pueda comprometer la seguridad de la Municipalidad de San Joaquín y sus recursos informáticos, como por ejemplo contagio de virus, intrusos, modificación o pérdida de datos y otras actividades poco usuales.
- No dejar información confidencial en los escritorios al alcance de todos.

Incumplimiento o violación de las políticas

Si se llegase a incumplir o violar una de estas políticas por parte del personal, el Jefe de Seguridad o encargado de Informática, realizará un informe detallado a la Directora de Gestión Administrativa o quien Subrogue. Este informe describirá la circunstancia y la gravedad del hecho y la Directora de Gestión Administrativa o quien subrogue deberá tomar las medidas necesarias sobre la persona implicada.

Estructura de la política

Está política se divide en las siguientes secciones:

- Seguridad física
- Seguridad lógica
- Seguridad en redes
- Planificación de contingencia y recuperación de desastres.

Cada sección se divide en tres partes:

Propósito: Define la intensión de cada sección
Alcance: Define el ámbito de aplicación
Controles generales: define los objetivos para cada sección.

POLÍTICA DE SEGURIDAD
FÍSICA

Propósito

El propósito de esta política preservar la seguridad de los recursos informáticos y garantizar la integridad y disponibilidad de los mismos.

Alcance

Estás políticas son aplicables a todos los recursos informáticos de la Municipalidad de San Joaquín entendiendo por ellos datos, hardware, software, personal e instalaciones.

Controles generales

1. Los computadores de la Municipalidad de San Joaquín sólo deben usarse en un ambiente seguro. Se considera que las oficinas de la municipalidad son un ambiente seguro porque en ellas se han implantado las medidas de control apropiadas para proteger datos, hardware, software, personal e instalaciones.
2. Toda persona debe portar credenciales de identificación.
3. Se deben mantener registros de entrada a la sala de servidores.
4. Se debe instalar videocámaras en la sala de servidores a fin de identificar personas ajenas a la organización.
5. El área de desarrollo deberá estar separada de la sala de servidores.
6. La temperatura de los equipos de aire acondicionado que abastecen al Departamento de Informática en su sala de servidores deberá estar entre los 18-19ºC.
7. En caso de que el equipo de aire acondicionado falle se deben contar con alternativas para solucionar este problema como equipos de respaldo o ventiladores de pedestales a fin de refrescar los equipos.
8. Debe respetarse y no modificar la configuración de hardware y software establecida por el Departamento de Informática, pues este cambio puede poner en riesgo la integridad y disponibilidad del equipo.
9. No se permite comer o beber mientras se está usando un computador.
10. La municipalidad debe contar con señalización de salidas de emergencia, prohibiciones de comer, fumar, beber alrededor de los equipos.
11. El departamento de Informática debe contar con una planilla donde se encuentren teléfonos de emergencia, para cualquier contingencia.
12. Deben protegerse los equipos de riesgos del medioambiente (por ejemplo, polvo, incendio y agua).
13. La temperatura de las oficinas con computadoras debe estar comprendida entre 18 y 21 grados centígrados y la humedad relativa del aire debe estar entre 45% y el 65%.
14. Deben existir conexiones independientes para los equipos de cómputo.
15. Los cables eléctricos deben ser puestos en paneles y canales resistentes al fuego.
16. Deben usarse reguladores de voltaje, equipos de protección como fuentes de poder ininterrumpibles (UPS).

17. Se debe contar con equipos de suministro de energía alternos en caso de fallas.
18. Instalarse alarmas en la sala de servidores así como detectores de humo.
19. Cualquier falla en los computadores o en la red debe reportarse inmediatamente ya que podría causar problemas serios como pérdida de la información o indisponibilidad de los servicios.
20. Deben protegerse los equipos para disminuir el riesgo de robo, destrucción, y mal uso. Las medidas que se recomiendan incluyen el uso de candados de seguridad.
21. Los servidores no pueden estar sobre pisos falsos.
22. Los servidores de red y los equipos de comunicación (módems, routers, switch, etc) deben estar ubicados en locales apropiados, protegidos contra daños y robo. Debe restringirse severamente el acceso a estos locales y a los cuartos de cableado a personas no autorizadas mediante el uso de cerraduras y otros sistemas de acceso.
23. Los equipos deben marcarse para su identificación y control de inventario. Los registros de inventario deben mantenerse actualizados.
24. No pueden moverse los equipos o reubicarlos sin permiso. Para llevar un equipo fuera de las dependencias municipales se requiere una autorización escrita.
25. La pérdida o robo de cualquier componente de hardware o programa de software debe ser reportada inmediatamente.
26. Se debe llevar un registro de entrada y salida de los equipos de las instalaciones de la municipalidad.
27. Los usuarios deben configurar el protector de pantalla para que se active al cabo de 15 minutos de inactividad y que requiera una contraseña al reasumir la actividad.
28. El usuario debe activar el protector de pantalla manualmente cada vez que se ausente de su oficina.
29. No está permitido llevar al sitio de trabajo computadoras portátiles (laptops) o cualquier equipo personal, y en caso de ser necesario se requiere solicitar la autorización correspondiente.
30. Los datos confidenciales que aparezcan en la pantalla deben protegerse de ser vistos por otras personas mediante disposición apropiada del mobiliario de la oficina y protector de pantalla. Cuando ya no se necesiten o no sean de utilidad, los datos confidenciales se deben borrar.
31. A menos que se indique lo contrario, los usuarios deben asumir que todo el software de la compañía está protegido por derechos de autor y cuenta con licencia de uso. Por tal razón es ilegal y está terminantemente prohibido hacer copias o usar ese software para fines personales.
32. Los usuarios no deben copiar a un medio removible (como un pendrive, disco duro portátil), el software o los datos residentes en las computadoras de la municipalidad, sin la aprobación previa de sus jefes superiores o encargado de Informática.
33. No pueden extraerse datos fuera del Municipio sin la aprobación previa de la jefatura próxima o encargado de Informática.
34. Siempre que sea posible, debe respaldarse y eliminarse información confidencial de los computadores y unidades de disco duro antes de que se les envíe a reparación, siempre que el servicio sea proporcionado por una empresa distinta al Departamento de Informática de San Joaquín.
35. No deben dejarse las impresoras desatendidas, sobre todo si se está imprimiendo (o se va a imprimir) información confidencial de la municipalidad.

MUNICIPALIDAD DE SAN JO
ENCARGADO
INFORMATICA
INFORMATICA

36. No se permite bajo ninguna circunstancia el uso de cualquiera de las computadoras con propósitos de ocio o lucro.
37. Se dará mantenimiento a los equipos de acuerdo a las especificaciones del proveedor.
38. Sólo el personal de mantenimiento debidamente autorizado debería realizar la reparación y servicio de los equipos.
39. Se deben mantener registros de los mantenimientos preventivos y correctivos, además de sospechas de falla y fallas reales.
40. Todos los equipos deben estar cubiertos por un seguro.
41. El encargado de Informática o a quien éste designe es el responsable de realizar respaldos de la información.
42. Cada día deberá efectuarse un respaldo completo de las bases de datos y el servidor repositorio denominado Público.
43. El Web master deberá realizar los respaldos de todos los sitios web que tengan relación con la Municipalidad de San Joaquín, así como las bases de datos involucradas en las mismas.
44. La información respaldada deberá ser almacenada en un lugar seguro y distante del sitio de trabajo.
45. Los respaldos deben estar debidamente etiquetados.
46. En el momento en que la información respaldada deje de ser útil a la municipalidad, dicha información deberá ser borrada antes de deshacerse del medio.
47. Para ayudar a restaurar los archivos no dañados o no infectados, deben hacerse copias de todo antes de su uso, y deben guardarse tales copias en un lugar seguro.
48. Las impresoras, fotocopiadoras deben estar situados en lugares de acceso restringido.
49. Los funcionarios deben archivar inmediatamente documentos que ya no van a utilizar y no dejarlos sobre sus escritorios.

MUNICIPALIDAD DE SAN JOAQUIN
ENCARGADO INFORMATICA
INFORMATICA

POLÍTICA DE SEGURIDAD
LOGICA

Propósito

Tiene como propósito controlar el acceso a la información y los procesos del negocio.

Alcance

Estás políticas son aplicables para todos los sistemas de información y datos de la municipalidad. Así mismo es aplicable a todos los usuarios de la entidad que hacen uso de los sistemas de información.

Controles generales

Cuentas

1. Se debe crear un documento en donde el empleado declare conocer las políticas y procedimientos de seguridad y se haga responsable del uso de su cuenta de usuario.
2. El usuario al recibir una nueva cuenta, debe firmar un documento de responsabilidad con el uso que le dé a su cuenta.
3. La solicitud de una nueva cuenta o el cambio de privilegios debe ser hecha por escrito al encargado de informática y debe ser debidamente aprobada por el respectivo Jefe de departamento o área.
4. Las cuentas deben ser otorgadas exclusivamente a usuarios legítimos.
5. Una cuenta deberá estar conformada por un nombre de usuario y su respectiva contraseña.
6. El nombre de usuario de una cuenta deberá estar conformado por la primera letra de su nombre y su apellido paterno, de existir alcances de nombre y apellido se procederá a crear con iniciales de primer y segundo nombre más el apellido.
7. Los privilegios de lectura, escritura, creación, eliminación y modificación de datos deben definirse de una manera consistente con las funciones que desempeña cada usuario.
8. Los privilegios del sistema concedidos a los usuarios deben ser ratificados cada 6 meses.
9. Privilegios especiales, tal como la posibilidad de modificar o borrar los archivos de otros usuarios, sólo deben otorgarse a aquellos directamente responsable de la administración o de la seguridad de los sistemas en cada Dirección municipal.
10. Toda cuenta queda automáticamente suspendida después de un cierto periodo de inactividad. El periodo recomendado es de 30 días.
11. Cuando un empleado es despedido, renuncia o sale de vacaciones de la municipalidad, debe desactivarse su cuenta antes de que deje el cargo, es responsabilidad de la Dirección municipal correspondiente dar aviso a informática o en su defecto Recursos Humanos.
12. La cuenta de un usuario es personal e intransferible, por lo cual no se permite que este comparta su cuenta ni su contraseña con persona alguna, aún si ésta acreditada la confianza del usuario.

Contraseñas

1. La longitud de una contraseña deberá siempre ser verificada de manera automática al ser construida por el usuario. Todas las contraseñas deberán contar con al menos seis caracteres.
2. La longitud de la contraseña serán de mínimo seis caracteres.
3. Todas las contraseñas elegidas por los usuarios deben ser difíciles de adivinar.
4. No deben ser utilizadas como claves palabras que aparezcan en el diccionario, secuencias conocidas de caracteres, datos personales ni acrónimos.
5. Está prohibido que los usuarios construyan contraseñas compuestas de algunos caracteres constantes y otros que cambien de manera predecible y sean fáciles de adivinar.
6. Los usuarios no deben construir contraseñas idénticas o muy parecidas a contraseñas anteriores.
7. El usuario no debe guardar su contraseña en una forma legible en archivos, disco y tampoco debe escribirla en papel y dejarla en sitios donde pueda ser encontrada.
8. Nunca debe compartirse la contraseña o revelarla a otros.
9. Las contraseñas deben ser encriptadas para imposibilitar su identificación.

Control de acceso

1. Todos los usuarios deberán acceder a los sistemas utilizando un login que permita una comunicación segura y encriptada.
2. Al momento de ingresar a los sistemas y al sistema operativo, cada usuario quedará registrado con la fecha, hora y dirección desde la que se conectó al sistema por última vez.
3. Para prevenir ataques, cuando los sistemas lo permitan, debe limitarse a 3 el número de intentos infructuosos de introducir la contraseña, luego de lo cual la cuenta involucrada queda suspendida y se alerta al Administrador del sistema.
4. Si no ha habido ninguna actividad en un terminal, PC o estación de trabajo durante un cierto periodo de tiempo específicamente 10 a 15 minutos, el sistema debe automáticamente borrar la pantalla y suspender la sesión.
5. Los usuarios no deben intentar violar los sistemas de seguridad y de control de acceso. Acciones de esta naturaleza se consideran violatorias de las políticas de la municipalidad, pudiendo ser causal de sumario administrativo.
6. Se deben establecer días y horas de trabajo para los usuarios dentro de todos los sistemas.

Aplicaciones

1. Está estrictamente prohibido hacer uso de programas que explotan alguna vulnerabilidad de un sistema para proporcionar privilegios no otorgados explícitamente por el administrador.
2. Está estrictamente prohibido hacer uso de herramientas propias de delincuentes informáticos, tales como programas que rastrean vulnerabilidades en sistemas de cómputos propios o ajenos.
3. Se deben generar registros del uso de las aplicaciones que contengan:
    - El identificador del usuario
    - Fecha y hora de conexión y desconexión
    - Identificación del terminal

- Registro de intentos aceptados y rechazados de acceso al sistema.
- Registro de los intentos aceptados y rechazados de acceso a datos y otros recursos.

4. Los archivos de bitácora (logs) y los registros de auditoria que graban los eventos relevantes sobre la seguridad de los sistemas informáticos, deben revisarse cada semana y guardarse durante un tiempo prudencial de por lo menos tres meses.
5. Para tener evidencias en casos de acciones disciplinarias y judiciales, cierta clase de información debe capturarse, grabarse y guardarse cuando se sospeche que se esté llevando a cabo abuso, fraude u otro acceso que ponga en riesgo a los sistemas informáticos.
6. Está terminantemente prohibido instalar programas de uso personal.

Problemas de seguridad lógica

1. Se debe implementar un sistema de manejo de problema de seguridad lógica en el que se registren y den seguimiento a todos los incidentes de seguridad lógica, inclusive las causas que lo provocaron.
2. El software de desarrollo y de producción deberán funcionar en servidores distintos.
3. Las tareas de desarrollo y producción deben estar separadas.
4. Los servicios del sistema no deben ser accesibles desde los sistemas de producción.
5. Se deben tener claves diferentes para el sistema de producción y el de desarrollo.

POLÍTICA DE SEGURIDAD
EN REDES

Propósito

El propósito de esta política es establecer las directrices, los procedimientos y los requisitos para asegurar la protección apropiada de la compañía al estar conectada a redes de computadoras.

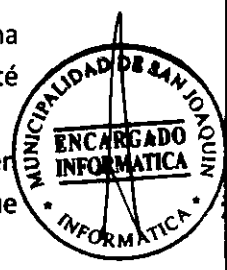
Alcance

Esta política se aplica a todos los funcionarios, y personal temporal del municipio.

Controles generales

Correo electrónico, Internet e Intranet.

1. Debe instalarse y activarse una herramienta antivirus, la cual debe mantenerse actualizada. Si se detecta la presencia de un virus u otro agente potencialmente peligroso, se debe notificar inmediatamente al departamento de Informática y poner la computadora en cuarentena hasta que el problema sea resuelto.
2. Sólo pueden bajarse archivos de redes externas de acuerdo a los procedimientos establecidos. Debe utilizarse un programa antivirus para examinar todo software que venga de afuera o inclusive de otros departamentos de la compañía.
3. No debe utilizarse software bajado de Internet y en general software que provenga de una fuente no confiable, a menos que este haya sido comprobado en forma rigurosa y que esté aprobado su uso por el Departamento de Informática.
4. No deben usarse pendrive u otros medios de almacenamiento como discos duros externos en cualquier computadora de la municipalidad a menos que se haya previamente verificado que están libres de virus u otros agentes dañinos.
5. El usuario es la única persona autorizada para leer su propio correo, a menos que su cuenta esté involucrada en un incidente de seguridad informática.
6. Está estrictamente prohibido usar la cuenta de correo electrónico proporcionada por la organización para propósitos ajenos a sus actividades laborales.
7. No se permite el uso de la cuenta de correo electrónico para suscribirse a listas electrónicas de discusión de interés personal.
8. El firewall será programado para dar acceso sólo a páginas que cada usuario por sus funciones tendrá permitido acceder.



POLÍTICA DE PLANIFICACIÓN DE CONTINGENCIA Y RECUPERACIÓN DE DESASTRES

Propósito

Garantizar la continuidad de las operaciones de negocio de la municipalidad y limitar el impacto económico/financiero e intangible en el negocio en caso que se detecte un evento inesperado que ocasione la interrupción de las operaciones de la compañía.

Alcance

Esta política se aplica a todos los sistemas de información y datos de la compañía.

Controles generales

1. *El plan de contingencia debe ser realizado y sometido a prueba por el Jefe de seguridad o encargado de Informática y junto a la ayuda del personal seleccionado para el plan. Este plan deberá ser aprobada toda su ejecución por la Administración Municipal.*
2. *Deben proveerse procedimientos de contingencia para los sistemas del negocio que incluyan niveles definidos y documentados de recuperación en el caso de desastres o fallas de sistemas.*
3. *Se debe proteger primero al personal como recurso fundamental en cualquier contingencia.*
4. *Deben ponerse a prueba tales planes en un intervalo de seis meses. Las actividades de planificación de contingencia deben ser coordinadas y administradas en forma centralizada.*
5. *Se deben identificar los registros esenciales y hacer los arreglos adecuados para mantener copias de tales registros en las sedes alternativas donde se trabajará en caso de eventos inesperados.*
6. *Las Redes alternativas no deben estar ubicadas en el mismo lugar donde se encuentre el Servidor Central.*
7. *Debe disponerse de una copia completa de la documentación requerida, el software de base, software de aplicaciones y datos en producción, así como los registros (logs) de transacciones que permitan restaurar los datos o información en caso de pérdidas o daños.*
8. *Las copias de resguardo de los sistemas principales, los datos de registros esenciales y la documentación de Tecnología Informática, deben ser almacenadas teniendo en cuenta las políticas de seguridad física.*
9. *Deben registrarse y resguardarse los registros históricos que contabilicen los medios de almacenamiento de copias de resguardos que se mantienen en las sedes remotas de almacenamiento.*
10. *Se deben establecer planes de contingencias detallados que definan las acciones que han de tomarse y el personal requerido, para realizar la recuperación de los sistemas del negocio.*
11. *En el plan debe definirse quién es el responsable de su ejecución y detallar las funciones que las personas involucradas en el plan deben tener.*
12. *El plan de contingencia deberá ser conocido por toda la organización.*
13. *Dichos planes deben ser revisados y actualizados cada seis meses.*